TEMEL BİLGİ GÜVENLİĞİ-6

Denial Of Service (DoS)-Servis Sonlandırma Saldırıları

DoS saldırıları genel olarak sistemleri çalışamaz hale getirmek için yapılan saldırılardır. DoS saldırıları internet üzerinden gerçekleştirilebileceği gibi, ağ yapısı olan tüm ortamlar üzerinde gerçekleştirilebilir. Yani kablosuz ağlar ve yerel ağlarda DoS saldırılarının tehdit ettiği ortamlardır.

DoS saldırıları tek bir makinadan gerçekleştirilebilir yada bir saldırıyı gerçekleştirmek için birden çok bilgisayar/bileşen kullanılabilir. En çok karşılaştığımız haber türlerinden olan bilinen hacker grupların saldırıları DoS saldırıları şeklinde gerçekleşebilmektedir. Bu türden saldırılarda çoğunlukla roBOTNETworks (botnet)' ler kullanılmakta ve dağıtık servis sonlandırma saldırıları şeklinde gerçekleştirilmektedir. (distrubuted denial of service-DDOS). Bu saldırı türünde bir çok farklı bileşen tek bir hedefin kaynaklarını tüketerek saldırılarını gerçekleştirir.

DoS saldırılarında hedef genellikle gizli bilgilerin ele geçirilmesi yada güvenlik kaybı değildir. Saldırılarda amaçlanan genellikle kişinin yada şirketin/kurumun prestij, zaman ve para kaybetmesidir. Saldırılardan etkilenen sistemlerde dosya ve programlarda zarar görebilmektedir.

Spyware (Casus Yazılımlar)

Spyware (Casus Yazılımlar) izin almaksızın, reklam verme, kişisel bilgi toplama yada bilgisayar konfigürasyonunu değiştirme davranışlarında bulunan, adware yada önemli verileri takip eden yazılımlardır.

Spyware'ler web siteleri üzerinden bir pop-up mesajıyla çıkan yükleme bildirimine izin verilmesi yada bilgilendirme olmaksızın programın bilgisayara yüklenmesi ile bulaşabilir.

Spyware programı bilgisayara bulaştıktan sonra, gerçekleştirilen aktiviteleri izler ve üçüncü taraflarla paylaşımda bulunur. Spyware çalışırken bilgisayarı yavaşlatabilir, çalışamaz hale getirebilir. Antivirüs yazılımları ile bu tür zararlı yazılımların temizlenmesi mümkündür.

Brute Force Attack

Brute Force (Deneme/Yanılma) saldırıları bir sisteme yada dosyaya yetkisiz erişebilmek için kullanıcı adı ve parolalarda çok sayıda numara ve karakter kombinasyonlarını deneyen saldırı türüdür. Saldırı süreleri kullanıcı bilgilerinin kompleks olma durumuna göre değişmektedir. Brute Force saldırılarını engellemenin yolu ise parola ve şifrelerin güvenli seçilmesidir. Bunu gerçeklemek için yeterince güçlü, en az bir sayı, özel karakter, büyük ve küçük harf içeren parolalar seçilmelidir. Bu parolalar mümkün olduğunca uzun olmalı ve kişisel bilgilerle tahmin edilebilir olmamalıdır. Bunu sağlamak için kullanılan arabaların plakaları, yakınlarımızın doğum tarihi, isim bilgileri, futbol takımı, şehir, popüler müzik ve kitap isimleri parola olarak seçilmemesi tavsiye edilmektedir. Ayrıca seçilen parolalar belirli periyotlarla güncellenmelidir.